UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/539,846 | 06/20/2005 | Toshihiko Ogihara | 44471/317116 | 5015 |

23370 7590 01/28/2009

JOHN S. PRATT, ESQ
KILPATRICK STOCKTON, LLP
1100 PEACHTREE STREET
ATLANTA, GA 30309

| EXAMINER | |
|---|---|
| SMITHERS, MATTHEW | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2437 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 01/28/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/539,846 | OGIHARA ET AL. | |
| | Examiner | Art Unit | |
| | Matthew B. Smithers | 2437 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *20 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/20/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Information Disclosure Statement*

The information disclosure statement filed June 20, 2005 has been placed in the application file and the information referred to therein has been considered as to the merits.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-12 are rejected under 35 U.S.C. 102(e) as being anticipated by US 6,996,724 granted to Murakami et al.

Regarding claim 1, Murakami meets the claimed limitations as follows: "A data division method for dividing original data into as many divided data as a desired number of division by using a prescribed processing unit bit length, comprising the steps of: generating a plurality of original partial data by dividing the original data by the prescribed processing unit bit length; generating a plurality of random number partial data each having a length equal to the

prescribed processing unit bit length, from a random number having a length less than or equal to a bit length of the original data, in correspondence to the plurality of original partial data; generating a plurality of divided partial data that constitute each divided data by using exclusive OR calculation of the original partial data and the random number partial data, each divided partial data having a length equal to the prescribed processing unit bit length; and generating the divided data in the desired number of division from the plurality of divided partial data, such that the original data cannot be ascertained from any one divided data alone but the original data can be recovered from a prescribed number of the divided data among generated divided data." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 2, Murakami meets the claimed limitations as follows: "The data division method of claim 1, wherein the original partial data and the random number partial data are generated as many as the desired number of division minus one." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 3, Murakami meets the claimed limitations as follows: "The data division method of claim 1, wherein the divided data include one or more divided data formed by a random number alone, and one or more divided data formed by the divided partial data generated by the exclusive OR calculation of one or more original partial data and one or more random number partial data." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 4, Murakami meets the claimed limitations as follows:

"The data division method of claim 3, wherein the one divided data formed by a random number alone is formed by repeating a random number with an arbitrarily determined length." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 5, Murakami meets the claimed limitations as follows: "The data division method of claim 3, wherein the one divided data formed by a random number alone is formed by a pseudo-random number generated from information of a prescribed length according to a pseudo-random number generation algorithm." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 6, Murakami meets the claimed limitations as follows: "The data division method of claim 1, wherein the divided data include two or more divided data formed by the divided partial data generated by the exclusive OR calculation of one or more original partial data and one or more random number partial data." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 7, Murakami meets the claimed limitations as follows: "The data division method of claim 1, wherein when the original data, the random number, the divided data, the desired number of division and the processing unit bit length are denoted as S, R, D, n and b, respectively, variables i (=1 to n) and j (=1 to n-1) are used as variables, each one of (n-1) sets of the original partial data, (n-1) sets of the random number partial data, n sets of the divided data D, and (n-1) sets of divided partial data of each divided data are denoted as S(j),

R(j), D(j), and D(i,j), respectively, each original partial data S(j) is generated as b bits of data from b.times.(j-1)+1-th bit of the original data S while changing a variable j from 1 to n-1, U[n,n] is an n.times.n matrix with u(i,j) indicating a value of i-th row and j-th column given by: u(i,j)=1 when i+j.ltoreq.n+1 u(i,j)=0 when i+j>n+1 P[n,n] is an n.times.n matrix with p(i,j) indicating a value of i-th row and j-th column given by: p(i,j)=1 when j=i+1 p(i,j)=1 when i=1, j=n p(i,j)=0 otherwise c(j,i,k) is defined as a value of i-th row and k-th column of an (n-1).times.(n-1) matrix U[n-1,n-1].times.P[n-1,n-1] (j-1), where U[n-1,n-1].times.P[n-1,n-1] (j-1) denotes a product of a matrix U[n-1,n-1] and (j-1) sets of a matrix .times.P[n-1,n-1], and Q(j,i,k) is defined as Q(j,i,k)=R(k) when c(j,i,k)=1 and Q(j,i,k)=0 when c(j,i,k)=0, each divided partial data D(i,j) is generated by: D .function. ( i , j ) = S .function. ( j ) * ( k = 1 n - 1 .times. .times. Q .function. ( j , i , k ) ) .times. .times. when .times. .times. i < n D .function. ( i , j ) = R .function. ( j ) .times. .times. when .times. .times. i = n while changing a variable i from 1 to n and changing a variable j from 1 to n-1 for each, variable i, where k = 1 n - 1 .times. .times. Q .function. ( j , i , k ) = Q .function. ( j , i , 1 ) * Q .function. ( j , i , 2 ) * .times. .times. * Q .function. ( j , i , n - 1 ) and * denotes the exclusive OR calculation." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 8, Murakami meets the claimed limitations as follows: "The data division method of claim 1, wherein each divided data is generated such that a random number component cannot be eliminated by carrying out calculation among the divided partial data that constitute the each divided data." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 9, Murakami meets the claimed limitations as follows: "The data division method of claim 8, wherein each divided data is generated by first generating the plurality of divided partial data that constitute each divided data by using a prescribed definition formula formed by the exclusive OR calculation of the original partial data and the random number partial data, and then interchanging one divided partial data and another divided partial data among the divided partial data that constitute each divided data." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 10, Murakami meets the claimed limitations as follows: "The data division method of claim 8, wherein each divided data is generated by first generating the plurality of divided partial data D(i,j) that constitute each divided data D(i) by using a prescribed definition formula formed by the exclusive OR calculation of the original partial data and the random number partial data, and then removing a j-th random number partial data R(j) from D(i,j) with a value of i in a range of n-1>i>0, where n is the desired number of division, j=(n-1).times.m+1, and m.gtoreq.0 is an arbitrary integer." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 11, Murakami meets the claimed limitations as follows: "A data division device for dividing original data into as many divided data as a desired number of division by using a prescribed processing unit bit length, comprising: an original partial data generation unit configured to generate a plurality of original partial data by dividing the original data by the prescribed processing unit bit length; a random number generation unit configured to

generate a plurality of random number partial data each having a length equal to the prescribed processing unit bit length, from a random number having a length less than or equal to a bit length of the original data, in correspondence to the plurality of original partial data; a divided partial data generation unit configured to generate a plurality of divided partial data that constitute each divided data by using exclusive OR calculation of the original partial data and the random number partial data, each divided partial data having a length equal to the prescribed processing unit bit length; and a divided data generation unit configured to generate the divided data in the desired number of division from the plurality of divided partial data, such that the original data cannot be ascertained from any one divided data alone but the original data can be recovered from a prescribed number of the divided data among generated divided data." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

Regarding claim 12, Murakami meets the claimed limitations as follows: "A computer program product for causing a computer to function as a data division device for dividing original data into as many divided data as a desired number of division by using a prescribed processing unit bit length, the computer program product comprising: a first computer program code for causing the computer to generate a plurality of original partial data by dividing the original data by the prescribed processing unit bit length; a second computer program code for causing the computer to generate a plurality of random number partial data each having a length equal to the prescribed processing unit bit length, from a random number having a length less than or equal to a bit length of the original

data, in correspondence to the plurality of original partial data; a third computer program code for causing the computer to generate a plurality of divided partial data that constitute each divided data by using exclusive OR calculation of the original partial data and the random number partial data, each divided partial data having a length equal to the prescribed processing unit bit length; and a fourth computer program code for causing the computer to generate the divided data in the desired number of division from the plurality of divided partial data, such that the original data cannot be ascertained from any one divided data alone but the original data can be recovered from a prescribed number of the divided data among generated divided data." Column 6, line 25 to column 8, line 19 and Figures 2, 3 and 4.

## *Conclusion*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Nadooshan et al (US 20030147535) discloses a method for multi-threshold secret sharing.

B. Watanabe et al (US 20020097868) discloses a method for encrypting using a pseudorandom number generating apparatus.

C. Miyazaki et al (US 6,810,122) discloses a secret sharing system.

D. Akiyama et al (US 5,623,548) discloses a transformation and an encryption device.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew B Smithers/
Primary Examiner, Art Unit 2437